明　細　書

情報保護システム、それに使用する記憶媒体及び記憶媒体収納ケース

技術分野

本発明は、低コスト且つ簡単な構成でハッカーの侵入阻止や記憶媒体内に格納されているデータを保護する情報保護システム、それに使用する記憶媒体及び記憶媒体収納ケースに関する。

背景技術

近年、あらゆるビジネス分野、医療・福祉分野を含め生活全般の電子化、通信のネットワーク化が促進され、その利便性は著しく向上している。この電子化に伴い、各種情報は一般にはパソコン内蔵の記憶媒体に格納され、記憶媒体としても多種多様な記憶媒体が使用されている。記憶容量が大きく価格的にも手ごろなハードディスク（ＨＤＤ）が最も広く用いられているが、記憶容量だけでなく携帯性と価格面、更には素材がプラスティックで廃棄に際して環境汚染の問題のない点を考慮すると最近は光ディスクが有望なメモリ媒体として注目されている。

ところで、近年、全国の地方自治体と中央をネットワークで接続し、市町村のもつ住民の個人情報をデータベース化して全国どこからでも当該データベースから所望の情報を取得できるようにした住基ネットワークの構築が進んでいる。

かかる住基ネットワークは、各市町村等の自治体に、ファイアウォールを設けたコミュニケーションサーバーを設置し、既存の住基管理システムに接続するとともに、このコミュニケーションサーバーと各都道府県、東京の地方自治情報センターに設置したサーバーとを専用回線で接続し、中央や地方の行政機関が、必要に応じて情報を授受するような構成を基本とする。

この種のネットワークでは、個人情報という機密情報を扱うため、そのセキュリティは高度なものでなければならない。一方、一部の市町村では、庁内ＬＡＮがファイアウォールを介してインターネットに接続されており、インターネットを介

してシステムに侵入される恐れがある。したがって、一旦、システムに侵入されてしまうと、そこからネットワーク全体への侵入の恐れも生ずることになる。

かかる問題を解決するため、市町村のコミュニケーションサーバーのファイアウォールから内側のネットワークでは独自開発されたプロトコルが使用されたり、サーバーで使用されるアプリケーションも独自開発する等の対策が施されているが、市町村レベルで独自開発されたプロトコルやアプリケーションは比較的大規模にならざるを得ず、一旦破られると、新たなプロトコルやアプリケーションを開発することになり、ハッカーとのいたちごっこに陥ってしまうことになる。

このような問題は、勿論、住基ネットワークに限られるものではなく、同様なネットワークや記憶媒体にも生ずる。

上述のように、従来のインターネットに接続されているネットワークはファイアウォールが設置されているとしてもハッカーによる侵入を完全に阻止できるものではない。

そこで、本発明の目的は、ハッカーの侵入阻止や個別記憶媒体内に格納されているデータを保護する簡易で低コストな情報保護システム、それに使用する記憶媒体及び記憶媒体収納ケースを提供することにある。

発明の開示

前述の課題を解決するため、本発明による情報保護システム、それに使用する記憶媒体及び記憶媒体収納ケースは次のような特徴的な構成を有する。

（1）情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有するとともに、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体が、外部装置に装着され、前記外部装置から前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可ＯＫのときのみアクセスを可能とする情報保護システム。

（２）情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有するとともに、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体が装着された外部装置を複数備え、且つ前記記憶媒体に記憶されている許可情報のいずれかは異なっており、前記外部装置から前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可ＯＫのときのみアクセスを可能とする情報保護システム。

（３）専用回線で接続されたパソコンを有する独立ネットワークと、ＬＡＮ接続された複数のパソコンを有し、インターネットに接続された通常ネットワークとが接続されたネットワークシステムにおいて、

前記通常ネットワークの各パソコンに、情報データと少なくともパソコンを制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記パソコンを制御する電子回路部とを有し、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体が装着され、前記パソコンから前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可されたときのみアクセスを可能とする情報保護システム。

（４）情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有するとともに、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている複数個の記憶媒体が収納ケースに収納され、予め登録された特定人であることを認証したときのみ所定の記憶媒体が前記記憶媒体収納ケースからの取り出しが可能とされ、

前記取り出された記憶媒体が外部装置に装着され、前記外部装置から前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可ＯＫのときのみアクセスを可能とすることを特徴とする情報保護システム。

（５）情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有するとともに、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている複数個の記憶媒体が収納ケースに収納され、予め登録された特定人であることを認証したときのみ所定の記憶媒体が前記記憶媒体収納ケースからの取り出しが可能とされ、

前記取り出された記憶媒体が複数個の外部装置に装着され、且つ前記記憶媒体に記憶されている許可情報のいずれかは異なっており、前記外部装置から前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可ＯＫのときのみアクセスを可能とする情報保護システム。

（６）専用回線で接続されたパソコンを有する独立ネットワークと、ＬＡＮ接続された複数のパソコンを有し、インターネットに接続された通常ネットワークとが接続されたネットワークシステムにおいて、

前記通常ネットワークの各パソコンに、情報データと少なくともパソコンを制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記パソコンを制御する電子回路部とを有し、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体が収納ケースに収納され、予め登録された特定人であることを認証したときのみ所定の記憶媒体が前記記憶媒体収納ケースからの取り出しが可能とされ、

取り出された記憶媒体が外部装置に装着され、前記パソコンから前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可されたときのみアクセスを可能とする情報保護システム。

（７）前記外部装置はパソコンであり、インターネットに接続されている上記（１）乃至（６）のいずれかの情報保護システム。

（８）前記認証結果がＮＧであるときに記憶媒体が取り出されたときには、警報告知を行う手段を有する上記（１）乃至（６）のいずれかの情報保護システム。

（９）前記認証がＮＧであるときに記憶媒体が取り出され、且つ予め定めた範囲外に移動したときに警報告知を行う手段を有する上記（４）乃至（６）のいずれかの情報保護システム。

（１０）前記警報告知は、通信回線を介して管理センターに送信される上記（４）乃至（６）のいずれかの情報保護システム。

（１１）前記複数の外部装置に装着された記憶媒体に記憶されている許可情報のいずれかは異なっている上記（２）または（５）の情報保護システム。

（１２）前記記憶媒体に記憶されている情報データは暗号化されており、前記許可情報は前記暗号化を解読するための情報である上記（１）乃至（１１）のいずれかの情報保護システム。

（１３）前記記憶媒体は、光ディスクである上記（１）乃至（１２）のいずれかの情報保護システム。

（１４）外部装置に着脱可能で、情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有し、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体。

（１５）前記記憶媒体に記憶されている情報データは暗号化されており、前記許可情報は前記暗号化を解読する情報である上記（１４）の記憶媒体。

（１６）上記（１４）または（１５）の記憶媒体の記憶部に対する読み／書きアクセスするとともに前記電子回路部との通信を行うインタフェース部を有するドライブが、前記記憶媒体と一体化されて成る記憶媒体ドライブユニット。

（１７）上記（１４）乃至（１６）「のいずれかの記憶媒体または記憶媒体ドライブユニットを複数個収納するとともに、予め登録された特定人であることを認証したときのみ所定の記憶媒体または記憶媒体ドライブユニットの取り出しを可能とした記憶媒体収納ケース。

（１８）前記認証はＩＤまたは生体認証である上記（１６）の記憶媒体収納ケース。

（１９）前記認証結果がＮＧであるときに記憶媒体が取り出されたときには、警報告知を行う手段を有する上記（１７）または（１８）の記憶媒体収納ケース。

（２０）前記認証がＮＧであるときに記憶媒体が取り出され、且つ予め定めた範囲外に移動したときに警報告知を行う手段を有する上記（１７）乃至（１９）のいずれかの記憶媒体収納ケース。

（２１）前記警報告知は、警告音または警告表示である上記（１９）乃至（２０）の記憶媒体収納ケース。

（２２）前記警報告知は、通信回線を介して管理センターに送信される上記（１９）乃至（２１）のいずれかの記憶媒体収納ケース。

（２３）前記記憶媒体は、光ディスクである上記（１４）乃至（２２）のいずれかの記憶媒体収納ケース。

（２４）前記記憶媒体はカートリッジに収容されている上記（１）乃至（２３）のいずれかの情報保護システム、記憶媒体または記憶媒体収納ケース。

（２５）前記カートリッジには、任意の記憶媒体を収容可能である上記（１）乃至（２３）のいずれかの情報保護システム、記憶媒体または記憶媒体収納ケース。

（２６）前記カートリッジには無線通信のための無線通信部、認証部、表示部、音声出力部、これら機能部動作のためのバッテリ部が搭載されている上記（２４）または（２５）の情報保護システム、記憶媒体または記憶媒体収納ケース。

（２７）前記無線通信部による無線通信により前記カートリッジの所在位置が管理され、所定範囲以外に前記カートリッジが持ち出されたときには警報が鳴り、また無線通信回線を介して警報センターに通報して異常を知らせる上記（２５）の情報保護システム、記憶媒体または記憶媒体収納ケース。

（２８）前記カートリッジに搭載した認証部により、当該カートリッジを取り出そうとする人が、登録されている利用を許可された人ではない（認証ＮＧ）場合には、警告を発し、または警報センターに通報する上記（２７）の情報保護システム、記憶媒体または記憶媒体収納ケース。

（２９）前記カートリッジの無線通信部と、前記記憶媒体側に設けた無線通信部により通信を行うことにより前記記憶媒体の妥当性を確認する上記（２７）の情報保護システム、記憶媒体または記憶媒体収納ケース。

（３０）前記記憶媒体は、光ディスクである上記（２４）乃至（２９）のいずれかの情報保護システム、記憶媒体または記憶媒体収納ケース。

本発明の情報保護システム、それに使用する記憶媒体及び記憶媒体収納ケースによると、次の如き実用上の顕著な効果が得られる。

すなわち、外部のハッカーがインターネットからパソコンに侵入できたとしても、また侵入できたパソコンにＬＡＮ接続された他のパソコンに侵入できたとしても、機密情報が格納されている記憶媒体（インテリジェントディスク）は、パソコンそのものを能動的に制御し、またパソコンに装着される個別のセキュリティプログラムにより守られているので、更なる障壁となり、機密情報は確実に保護される。このとき、セキュリティプログラムを個々のディスク毎に変えるだけでそれぞれ独立したセキュリティプログラムとして機能するので、プログラム開発も簡単に行える。更に、記憶媒体収納ケースに上記記憶媒体を複数個収納しておき、予め登録された特定人であることを認証したときのみ記憶媒体の取り出しを可能とし、認証がＮＧであるときに記憶媒体が取り出され、また予め定めた範囲外に移動したときには警報告知を行い、また通信回線を介して管理センターに送信することにより、記憶媒体そのものの管理、セキュリティも確実に行われるという効果を奏する。また、記憶媒体として光ディスクを用いれば低コストで記憶容量が大きく廃棄時の環境問題も生じない。

図面の簡単な説明

第１図は、本発明による情報保護システムの構成図である。

第２図Ａは、第１図に示す実施例の主要動作を説明するためのシステム図であり、インターネットを介して侵入された場合のパソコン側の記憶媒体に格納されている情報の読み出しが為されてしまう例の説明図である。

第２図Ｂは、第１図に示す実施例の主要動作を説明するためのシステム図であり、インターネットを介して侵入された場合の本発明によるインテリジェントディスクを用いて情報読み出しを阻止するシステムについての説明図である。

第３図は、本発明の実施例で使用されるインテリジェントディスクを簡略化して示す図である。

発明を実施するための最良の形態

以下、本発明による情報保護システム、それに使用する記憶媒体及び記憶媒体収納ケースの好適実施形態の構成および動作を、添付図面を参照して詳細に説明する。

第１図は、本発明の一実施例による情報保護システム構成図である。

自治体内業務ネットワーク１００には、住基・戸籍サーバー、税務・財務サーバー、基幹系サーバー等１１が設置され、それぞれにはバスを介して多数のパソコン１２～１４、１５Ａ、１５Ｂ、１６、１７が接続され、各サーバーが分担する業務処理が実行される。パソコン１２、１３及び１４は、それぞれＣＳ端末、住基端末及び財務端末を示し、当該業務専用の端末である。パソコン１５Ａと１５Ｂ、１６、１７は、業務用以外の汎用パソコンで、パソコン１６はスタッフが自己所有のパソコンを持ち込んで使用しているパソコン、パソコン１７は外出先から回線を介して自治体内業務ネットワーク１に接続されているパソコン１６にアクセスしてＬＡＮ回線を利用しているパソコン１７である。

自治体内業務ネットワークには、堅固なセキュリティが確保されている住基ネット仮想専用線ネットワークに接続されている住基ネットワーク２００がルータやファイアウォール（Ｆ／Ｗ）、ハブ（ＨＵＢ）を介して接続されている。

ところで、かかるシステムでは、自治体内業務ネットワークと住基ネットワークとの接続部分には、セキュリティ確保について十分な対策が施されていないため、インターネットに接続されている自治体内業務ネットワークには、インターネットを介して外部から侵入される恐れがある。

従来のシステムでは、個人情報データはパソコンに内蔵されているハードディスクまたは接続されているディスクに記憶されており、インターネットを介して自治体内業務ネットワークに侵入されると、パソコン内のハードディスクまたはそこに接続されているハードディスクへのアクセスの可能性が生ずる。その結果、ハードディスクに記憶されている個人情報が読み出されて外部に流出する恐れが発生することになる。

また、自治体内業務ネットワークに接続されているパソコンは、当該業務固有で使用されるパソコンだけでなく、上述のように、業務上の都合等で、時に担当者が持ち込んで使用する自己所有のパソコン１６のような一般パソコンが接続されることもある。業務用パソコンではセキュリティ面での特別な配慮が施されていることが多いが、一般パソコン１５Ａ、１５Ｂ、１６ではそのような配慮が為されていないため、ハッカーのような第三者の侵入の恐れが大きくなる。更に、外出先で使用するパソコン１７からのアクセス時にも同様な問題が生ずる。

本発明の実施例では、かかるインターネットを介しての侵入があっても個人情報等の情報の流出を防止するために、パソコン内蔵ではなく、パソコンに着脱可能な記録媒体としての光ディスク（以下、インテリジェントディスク：ｉ―ＤＩＳＣと称する）１Ａ、１Ｂを用いる。光ディスクは、他の記憶媒体と比較して、著しく低コストであるにもかかわらず記憶容量が格段に大きく、廃棄時の環境問題がない。インテリジェントディスク１Ａは、ドライブを一体化せず、装着されるパソコン側にドライブ装置が搭載されているパソコンに使用され、インテリジェントディスク１Ｂはディスクへのアクセス手段としてのドライブを一体化した一体化インテリジェントディスクである。

このインテリジェントディスクは、従来の光ディスクとは異なり、個人情報等の情報と所定のアプリケーションプログラムが記憶されている記憶部を有し、この記憶部に記憶されているアプリケーションプログラムに基づいて、当該光ディスクが装着されているパソコンの動作を制御する。その制御は、結局、当該光ディスクが装着されている外部装置としてのパソコン動作を制御するものである。すなわち、光ディスクに記憶されている情報の読み出し／書き込み等のアクセスを禁止させる

ようなアプリケーションプログラム（セキュリティ）を各光ディスク対応で記憶しておく。このプログラムは、光ディスクの記憶部に記憶する際の情報データの暗号化プログラム（暗号化キー等を含む）や光ディスクへのアクセスそのものを制御するプログラムでも良い。上記インテリジェントディスクには、個人情報等の機密情報を含む情報が記憶され、また処理された情報データも当該インテリジェントディスクに記憶される。したがって、たとえインターネットを介してハッカーが侵入したとしても、その侵入はパソコン止まりで、インテリジェントディスク内への侵入はできず、セキュリティが確保される。

第２図（Ａ）と（Ｂ）には、インターネットを介して侵入された場合のパソコン側の記憶媒体に格納されている情報の読み出しが為されてしまう従来のシステムと、本発明によるインテリジェントディスクを用いて情報読み出しを阻止するシステムについての説明図が示されている。

第２図（Ａ）において、ＬＡＮ接続され、それぞれセキュリティプログラムが搭載されている複数のパソコン１０Ａ～１０Ｃには通常簡単には侵入できない。しかしながら、これらのパソコンの１台１０Ａにセキュリティプログラムが搭載されていない場合には簡単に侵入できるし、セキュリティプログラムが搭載されていてもハッカーはインターネットを介して侵入することも多く、その場合、ＬＡＮ接続されている他のパソコン１０Ｂ、１０Ｃにも簡単に侵入されることになる。その結果、これらパソコンが利用するサーバーデータ２０に記憶されている個人情報等の機密情報が読み出され、外部に流出してしまう。

これに対して、本発明の実施例である第２図（Ｂ）では、上記インテリジェントディスク１がパソコンに装着されるような形態を採用しており、インテリジェントディスク１には、パソコン１０Ａ～１０Ｃのそれぞれの動作を規定する特有のプログラム（セキュリティプログラム）が格納されており、インテリジェントディスク１に格納されているプログラムで同インテリジェントディスク１からのデータ読み出しを制御するようにすれば、インターネットを介してようやく侵入してきたハッカーは更なる障壁に突き当り、この格別なセキュリティプログラムによる障壁を突き破ることはきわめて困難となる。また、インテリジェントディスク毎に異なる

特有プログラムを格納しておけば一つのパソコンのインテリジェントディスクに対して侵入できたとしても他のパソコンに装着されている別のセキュリティプログラムによる障壁を破る作業が更に必要であり、到底すべてのパソコンに装着されているインテリジェントディスクに格納されているデータを読み出すことは至難のわざである。

すなわち、本発明ではコンテンツ（インテリジェントディスク１に格納されている個人情報等のデータ）と、同インテリジェントディスク１に格納されているセキュリティプログラムが連動しており、またディスク毎に連動の態様が異なるるため、ディスク自体が堅固なセキュリティ機能を有することになる。したがって、パソコン等のハード側にファイアウォールやウイルス排除プログラム等のセキュリティが装備されていなくとも、インテリジェントディスク１自体がコンテンツを保護することになるため、そのセキュリティ機能は、従来と比較して極めてユニークで大きな効果を奏する。

セキュリティプログラムとして簡単なものはインテリジェントディスクに設けられた電子回路や外部装置としてのパソコンとの間でお互いを認識する認識コードを付与しておくようにすることができるし、インテリジェントディスクに記憶する情報データを暗号化しておき、この暗号化されたデータを読み出すためのキー情報に基づいて読み出せないようにしても良く、他に特別なセキュリティプログラムを設定することができる。

第３図は、インテリジェントディスク１の基本構造を示し、本例では２枚のディスクを張り合わせた構造を有し、片面側のディスク表面には個人情報等のデータを記憶する情報記憶部１０１が形成され、他面側のディスク表面にはパソコン制御プログラムやセキュリティプログラム等の情報を記憶するプログラム記憶部としてのＲＯＭ１０２と、ＲＡＭ部１０３と、上記プログラムを読み出してパソコンを制御する電子回路（ＣＰＵ）１０４と、この電子回路１０４と外部のパソコンやドライブ回路との信号授受のためのインタフェース部１０５と、外部との信号授受を無線で行うためのアンテナ部１０６とを備える。無線での信号授受は、例えば無線信号で行うことができるが、光信号で行うこともできる。

上述実施例の説明では、インテリジェントディスク１はディスク本体だけで構成され、ディスクに対するアクセスはパソコン側に設けたドライブにより行うが、第１図に示したようなディスクとドライブを一体化したインテリジェントディスク装置とすることもできる。この場合には、ディスクとドライブを有機的に結合した一体化構造とすることができるので、更なる固有性に富んだ装置が得られる。インテリジェントディスク装置は、パソコンにＰＣカード収納孔に挿入したり、ＵＳＢ接続するように構成することができる。

さて、第１図に戻ると、本実施例によるシステムは、上述のように、たとえ、ハッカーがインターネットを経由してネットワークに侵入できたとしても、ネットワーク内でＬＡＮ接続されているパソコンに接続されているインテリジェントディスクから機密情報を簡単に盗み出すことはできない。

本実施例では、更なるセキュリティ向上のため、インテリジェントディスクまたはインテリジェントディスク装置自体の利用を管理している。以下の説明ではインテリジェントディスク単体を管理する例について説明する。

自治体内業務ネットワークで使用する複数のインテリジェントディスクは、所定の収納場所で一括管理されている。収納場所は、人の出入りを厳密な管理し、許可された人のみ出入りでき、その入退出は記録管理されている。

多数のインテリジェントディスクは、鍵のかかる収納ケースに収納されており、その取り出しは、予め登録されている人のみが許可されている。取り出し時には、認証を必要とする。この認証は、収納ケースに設けられた認証手段により行われ、認証ＯＫであるときにのみ収納ケースからインテリジェントディスクを取り出せるようにしても良いし、インテリジェントディスク自体に認証手段を設けておき、認証ＯＫでなければ取り出せないようにすることもできる。認証手段としては、個人認証としての指紋認証等の生体認証やＩＤ認証等、任意の認証手法を用いることができる。認証ＮＧの場合には、その旨を警告するようにすることもできる。

このインテリジェントディスクの取り出しを許可された人として、当該部署の責任者を指定しておけば、より厳格な管理、セキュリティが確保される。すなわち、仕事開始前に責任者が、自己の認証が確認された後、必要なインテリジェントディ

スクを取り出し、部署内の担当者に渡して業務を開始する。その際、当該インテリジェントディスクに認証手段を設置しておき、担当者の認証を行うようにすることもできる。

ここで、収納ケースには液晶等の表示部を設けておき、認証時に認証された人の名前やインテリジェントディスクに付与した名称、認証ＮＧを示す警告等を表示させるようにすることができる。

また、第１図に示す実施例では、認証ＯＫを受けていない人Ｐが収納ケースやインテリジェントディスク１を持ち出そうとして、上記収納場所範囲Ｒから出ると、また、認証ＯＫを受けている人でも業務をする範囲（業務パソコン設置場所範囲）Ｒを越えると、警報が鳴ったり、警報信号が通信回線を介して警備会社等に送出され、警備処理が施される。警報信号は、高周波無線信号や光信号等の無線信号で送出される。こうして、重要な機密情報を記憶する記憶媒体が外部に持ち出されるような事態を防止することができる。更に、上記許容範囲外に持ち出されてしまった場合には、インテリジェントディスクに記憶されているデータ情報を壊す、消去するように設定することもできる。

上述実施例において、インテリジェントディスクは光ディスクそのものとして説明しているが、勿論、ディスクをカートリッジに収容しておいても良く、その場合には、カートリッジに各種機能部を搭載することができる。例えば、カートリッジに無線通信のための無線通信部、認証部、表示部、音声出力部（スピーカ）等及びこれら機能部動作のためのバッテリ部（充電可能なものが好ましい）を搭載することができる。無線通信部による無線通信によりカートリッジ（インテリジェントディスク）の所在位置が管理され、所定範囲（業務室）以外にインテリジェントディスクが持ち出されたときには警報が鳴り、また無線通信回線を介して警報センターに通報して、異常を知らせることができる。また、カートリッジに搭載した認証部により、当該カートリッジを取り出そうとする人が、登録されている利用を許可された人ではない（認証ＮＧ）場合には、同様に警告を発したり、警報センターに通報することができる。このような構成をとることにより、より確実な管理と被害の拡大を阻止することができる。カートリッジにはインテリジェントディスクが収

納されるが、インテリジェントディスクの取り出しや装着の自在構造とすれば、比較的高価なカートリッジを必要なときに所望のインテリジェントディスクに収納して共用することができる。すなわち、高価なシステムではカートリッジにインテリジェントディスクを固定的に収納しておき、汎用システムでは多数のインテリジェントディスクを一枚のカートリッジに共有することができる。

本実施例の他の例では、第３図に示すように、インテリジェントディスク側にも微弱無線通信を可能とするためのアンテナ部１０６が搭載されているため、カートリッジとの間の無線通信が可能となり、カートリッジ側とインテリジェントディスク側との通信によるインテリジェントディスクの妥当性を確認することができる。

以上の説明は、インターネットを介してパソコンに侵入する場合を想定して説明しているが、本発明は必ずしもインターネットを介する必要はなく、パソコン動作を介してそこに接続されている記憶媒体にアクセスして格納データを読み出すことを防止することができるものである。また、記憶媒体としても光ディスクに限定する必要はなく、同様な構成をもたせた記憶媒体を利用することもできる。

以上、本発明の好適実施形態例を説明したが、これは単なる例示にすぎず、特定用途に応じて種々の変形変更が可能であることは勿論である。

請 求 の 範 囲

1．情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有するとともに、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体が、外部装置に装着され、前記外部装置から前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可ＯＫのときのみアクセスを可能とすることを特徴とする情報保護システム。

2．情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有するとともに、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体が装着された外部装置を複数備え、且つ前記記憶媒体に記憶されている許可情報のいずれかは異なっており、前記外部装置から前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可ＯＫのときのみアクセスを可能とすることを特徴とする情報保護システム。

3．専用回線で接続されたパソコンを有する独立ネットワークと、ＬＡＮ接続された複数のパソコンを有し、インターネットに接続された通常ネットワークとが接続されたネットワークシステムにおいて、

前記通常ネットワークの各パソコンに、情報データと少なくともパソコンを制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記パソコンを制御する電子回路部とを有し、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体が装着され、

前記パソコンから前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可されたときのみアクセスを可能とすることを特徴とする情報保護システム。

４．情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有するとともに、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている複数個の記憶媒体が収納ケースに収納され、予め登録された特定人であることを認証したときのみ所定の記憶媒体が前記記憶媒体収納ケースからの取り出しが可能とされ、

前記取り出された記憶媒体が外部装置に装着され、前記外部装置から前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可ＯＫのときのみアクセスを可能とすることを特徴とする情報保護システム。

５．情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有するとともに、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている複数個の記憶媒体が収納ケースに収納され、予め登録された特定人であることを認証したときのみ所定の記憶媒体が前記記憶媒体収納ケースからの取り出しが可能とされ、

前記取り出された記憶媒体がそれぞれ複数個の外部装置に装着され、且つ前記記憶媒体に記憶されている許可情報のいずれかは異なっており、前記外部装置から前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可ＯＫのときのみアクセスを可能とすることを特徴とする情報保護システム。

６．専用回線で接続されたパソコンを有する独立ネットワークと、ＬＡＮ接続された複数のパソコンを有し、インターネットに接続された通常ネットワークとが接続されたネットワークシステムにおいて、

前記通常ネットワークの各パソコンに、情報データと少なくともパソコンを制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記パソコンを制御する電子回路部とを有し、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されている記憶媒体が収納ケースに収納され、予め登録された特定人であることを認証したときのみ所定の記憶媒体が前記記憶媒体収納ケースからの取り出しが可能とされ、

取り出された記憶媒体が外部装置に装着され、前記パソコンから前記記憶媒体へのアクセス時には、前記許可情報に基づいて許可されたときのみアクセスを可能とすることを特徴とする情報保護システム。

７．前記外部装置はパソコンであり、インターネットに接続されていることを特徴とする請求項１乃至６のいずれかに記載の情報保護システム。

８．前記認証結果がＮＧであるときに記憶媒体が取り出されたときには、警報告知を行う手段を有することを特徴とする請求項４乃至６のいずれかに記載の情報保護システム。

９．前記認証がＮＧであるときに記憶媒体が取り出され、且つ予め定めた範囲外に移動したときに警報告知を行う手段を有することを特徴とする請求項４乃至６のいずれかに記載の情報保護システム。

１０．前記警報告知は、通信回線を介して管理センターに送信されることを特徴とする請求項４乃至６のいずれかに記載の情報保護システム。

１１．前記複数の外部装置に装着された記憶媒体に記憶されている許可情報のいずれかは異なっていることを特徴とする請求項２または５に記載の情報保護システム。

１２．前記記憶媒体に記憶されている情報データは暗号化されており、前記許可情報は前記暗号化を解読するための情報であることを特徴とする請求項１乃至１１のいずれかに記載の情報保護システム。

１３．前記記憶媒体は、光ディスクであることを特徴とする請求項１乃至１２のいずれかに記載の情報保護システム。

１４．外部装置に着脱可能で、情報データと少なくとも外部装置を制御する所定のアプリケーションプログラムデータが格納されている記憶部と、この記憶部からデータを読み出し、読み出したアプリケーションプログラムに基づいて前記外部装置を制御する電子回路部とを有し、前記記憶部には更に前記記憶部へのアクセスを許可するか否かを制御する許可情報が格納されていることを特徴とする記憶媒体。

１５．前記記憶媒体に記憶されている情報データは暗号化されており、前記許可情報は前記暗号化を解読する情報であることを特徴とする請求項１４に記載の記憶媒体。

１６．請求項１４または１５に記載の記憶媒体の記憶部に対する読み／書きアクセスするとともに前記電子回路部との通信を行うインタフェース部を有するドライブが、前記記憶媒体と一体化されて成ることを特徴とする記憶媒体ドライブユニット。

１７．請求項１４乃至１６のいずれかの記憶媒体または記憶媒体ドライブユニットを複数個収納するとともに、予め登録された特定人であることを認証したときのみ所定の記憶媒体または記憶媒体ドライブユニットの取り出しを可能としたことを特徴とする記憶媒体収納ケース。

１８．前記認証はＩＤまたは生体認証であることを特徴とする請求項１６に記載の記憶媒体収納ケース。

１９．前記認証結果がＮＧであるときに記憶媒体が取り出されたときには、警報告知を行う手段を有することを特徴とする請求項１７または１８に記載の記憶媒体収納ケース。

２０．前記認証がＮＧであるときに記憶媒体が取り出され、且つ予め定めた範囲外に移動したときに警報告知を行う手段を有することを特徴とする請求項１７乃至１９のいずれかに記載の記憶媒体収納ケース。

２１．前記警報告知は、警告音または警告表示であることを特徴とする請求項１９または２０に記載の記憶媒体収納ケース。

２２．前記警報告知は、通信回線を介して管理センターに送信されることを特徴とする請求項１９乃至２１のいずれかに記載の記憶媒体収納ケース。

２３．前記記憶媒体は、光ディスクであることを特徴とする請求項１４乃至２２のいずれかに記載の記憶媒体収納ケース。

２４．前記記憶媒体はカートリッジに収容されていることを特徴とする請求項１乃至２３のいずれかに記載の情報保護システム、記憶媒体または記憶媒体収納ケース。

２５．前記カートリッジには、任意の記憶媒体を収容可能であることを特徴とする請求項１乃至２３のいずれかに記載の情報保護システム、記憶媒体または記憶媒体収納ケース。

２６．前記カートリッジには無線通信のための無線通信部、認証部、表示部、音声出力部、これら機能部動作のためのバッテリ部が搭載されていることを特徴とする請求項２４または２５に記載の情報保護システム、記憶媒体または記憶媒体収納ケース。

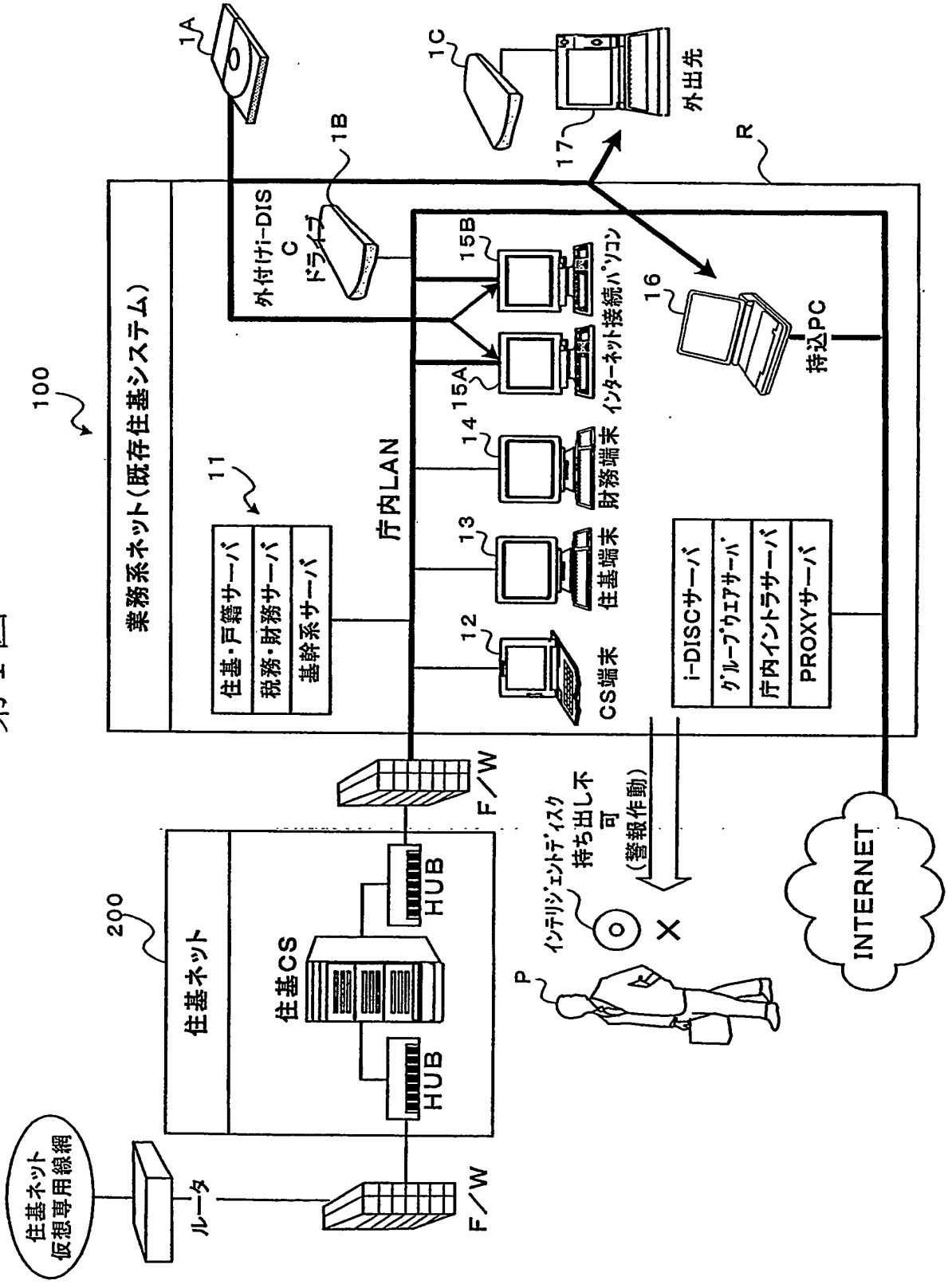
２７．前記無線通信部による無線通信により前記カートリッジの所在位置が管理され、所定範囲以外に前記カートリッジが持ち出されたときには警報が鳴り、また無線通信回線を介して警報センターに通報して異常を知らせることを特徴とする請求項２５に記載の情報保護システム、記憶媒体または記憶媒体収納ケース。

２８．前記カートリッジに搭載した認証部により、当該カートリッジを取り出そうとする人が、登録されている利用を許可された人ではない（認証ＮＧ）場合には、警告を発し、または警報センターに通報することを特徴とする請求項２７に記載の情報保護システム、記憶媒体または記憶媒体収納ケース。

２９．前記カートリッジの無線通信部と、前記記憶媒体側に設けた無線通信部により通信を行うことにより前記記憶媒体の妥当性を確認することを特徴とする請求項２７に記載の情報保護システム、記憶媒体または記憶媒体収納ケース。

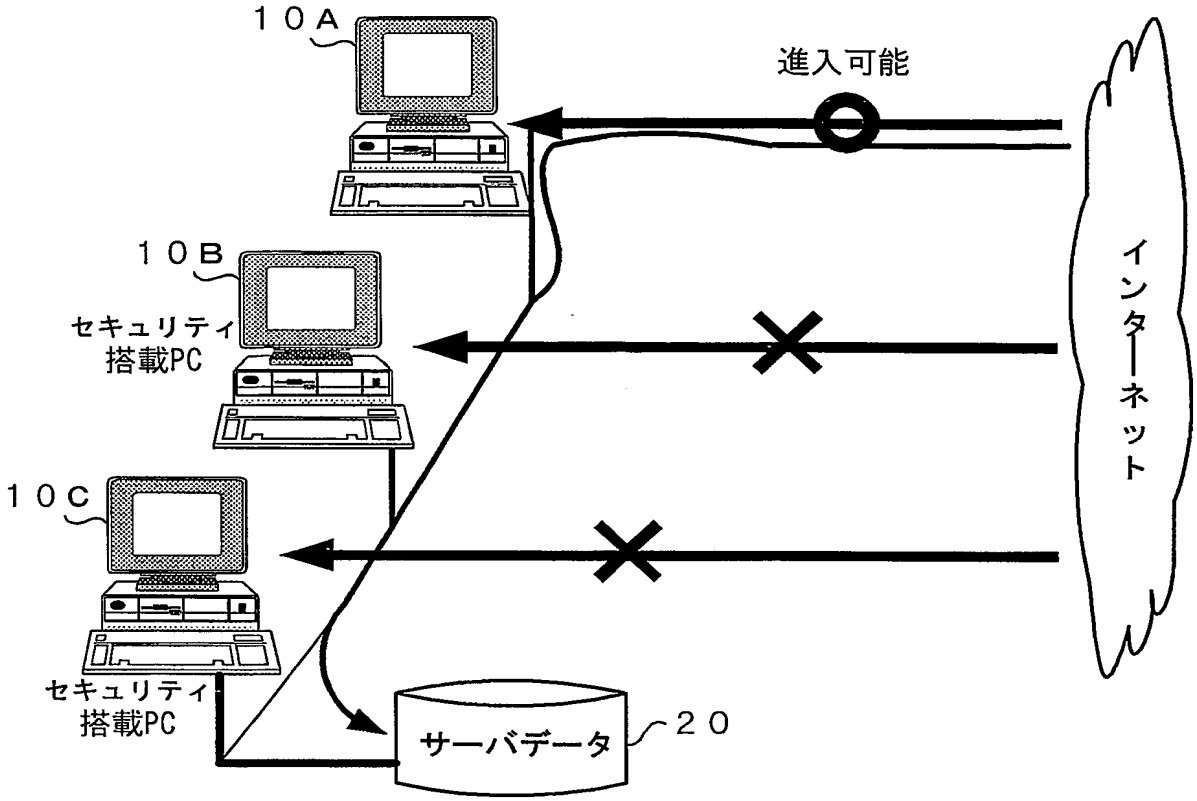
３０．前記記憶媒体は、光ディスクであることを特徴とする請求項２４乃至２９のいずれかに記載の情報保護システム、記憶媒体または記憶媒体収納ケース。

第1図



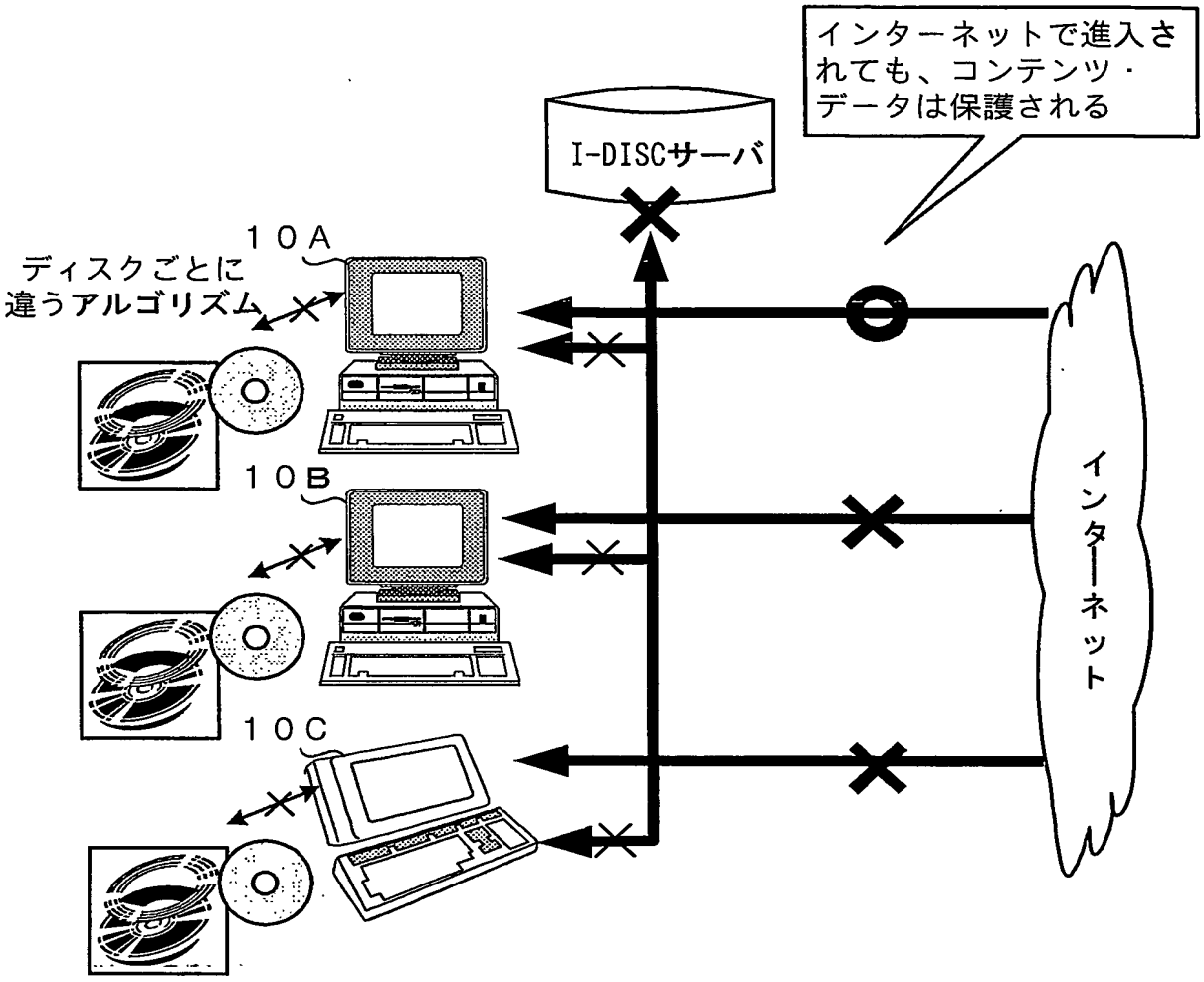
差替え用紙(規則26)

第２図



差替え用紙（規則26）

第３図


インターネットで進入されても、コンテンツ・データは保護される
I-DISCサーバ
１０Ａ
ディスクごとに違うアルゴリズム
１０Ｂ
１０Ｃ
インターネット

第４図